KATHOLIEKE UNIVERSITEIT LEUVEN

Open e-ID implementation for temporary and future card deployments

Gauthier Van Damme Karel Wouters Danny De Cock

Katholieke Universiteit Leuven
ESAT/SCD/IBBT-COSIC

World e-ID Conference, 2010

Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

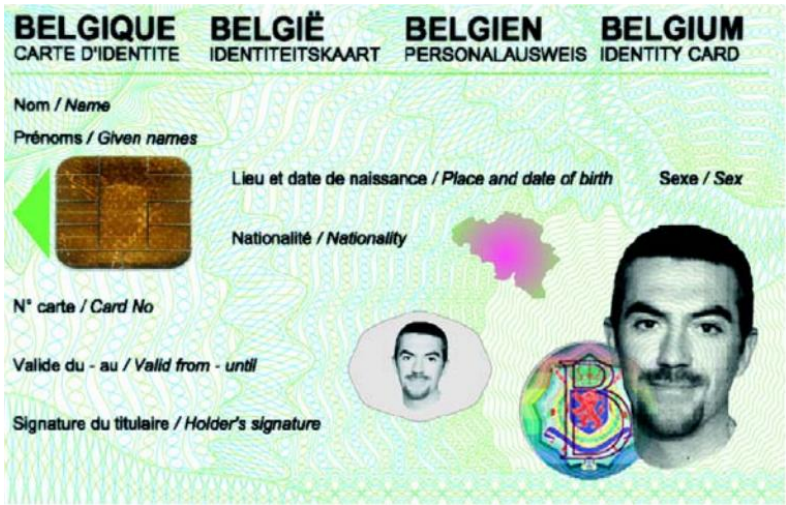
The Belgian e-ID card

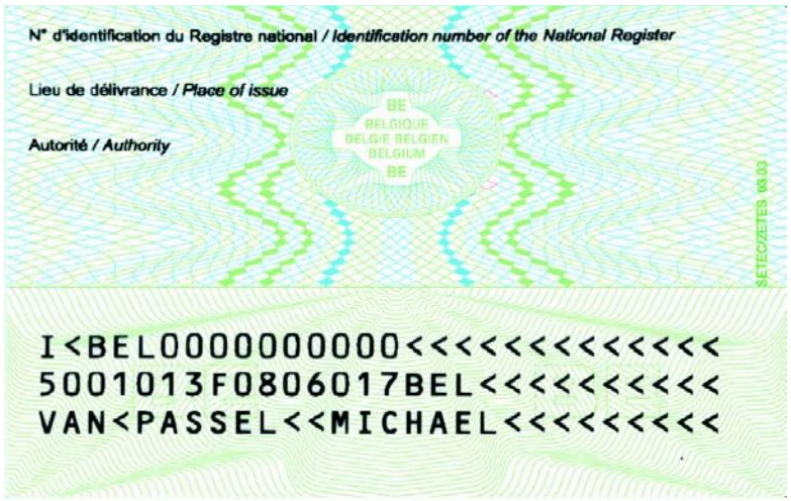
KATHOLIEKE UNIVERSITEIT LEUVEN

- March 31st, 2003: first Belgian e-ID cards issued
- Today: almost 10 million cards active
  - Mandatory for all citizens older than 12
  - Optional for all children younger than 12
  - Optional for all foreigner living in Belgium

Visual Aspects

- Printed information provide for normal citizen identification
- Only basic biometrics: citizen photo and signature
- International Civil Aviation Organization (ICAO) specified zone for border control
- Visual security mechanisms for card integrity verification





Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

The e-ID chip

- Based on Java Card technology
- Uses on-board key-pair generation
  - RSA 1024 and 2048 bit key operations using dedicated co-processor
  - Private keys do not leave the chip
  - Key-pair generation activated during e-ID card initialization
- Is managed by the Belgian government
  - Citizen data in the chip is read only after government initialization
  - Card rejects updates if not from the government

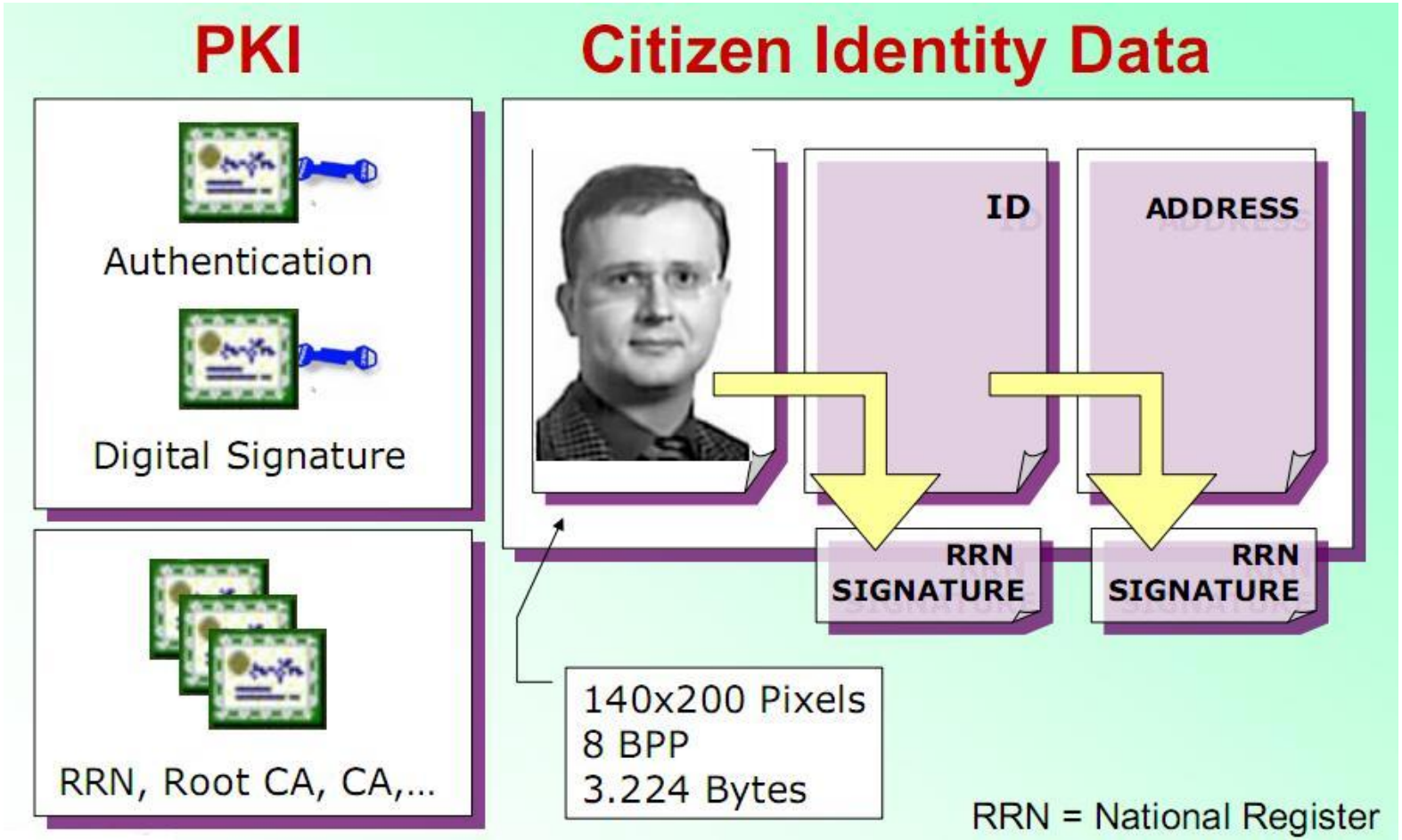
The e-ID chip functionalities

KATHOLIEKE UNIVERSITEIT LEUVEN

- The Belgian government established a PKI based on X.509 v3 certificates
- Two key pairs per citizen are defined inside this PKI
  - Authentication key pair for client authentication
  - Non-Repudiation key pair for file signature
- The use of the private keys require PIN entry, chosen by the citizen
- Compliant to the European Directive 1999/93/EC on equivalence with handwritten signatures
- A third key pair, without certificate, is used for card authentication by National Register (RRN)

The e-ID chip content

PKCS#12 file structure for content representation



Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

Current Use Cases

- eGovernment:
  - Official document request: marital status, birth certificate, ...
  - Access to RNN database
- eTax:
  - Online tax form declaration and consultation
  - 2,2 million tax-on-web declarations in 2010
- eAccess
  - Client authentication for web servers (e.g. eBay)
  - Access control to swimming pool, public library, civic amenity site
  - Age control (e.g. vending machines)
- eCommerce
  - Online account opening
  - Digital Rights Management
  - Qualified signature
- eHealth
  - Access to patient health record

Current Use Cases

- eGovernment:
  - Official document request: marital status, birth certificate, ...
  - Access to RNN database
- eTax:
  - Online tax form declaration and consultation

  - 2,2 million tax-on-web declarations in 2010
- eAccess
  - Client authentication for web servers (e.g. eBay)
  - Access control to swimming pool, public library, civic amenity site
  - Age control (e.g. vending machines)
- eCommerce
  - Online account opening
  - Digital Rights Management
  - Qualified signature
- eHealth
  - Access to patient health record

Current Use Cases

- eGovernment:
  - Official document request: marital status, birth certificate, ...
  - Access to RNN database
- eTax:
  - Online tax form declaration and consultation

  - 2,2 million tax-on-web declarations in 2010
- eAccess
  - Client authentication for web servers (e.g. eBay)
  - Access control to swimming pool, public library, civic amenity site
  - Age control (e.g. vending machines)
- eCommerce
  - Online account opening
  - Digital Rights Management
  - Qualified signature
- eHealth
  - Access to patient health record

Current Use Cases

- eGovernment:
  - Official document request: marital status, birth certificate, ...
  - Access to RNN database
- eTax:
  - Online tax form declaration and consultation

  - 2,2 million tax-on-web declarations in 2010
- eAccess
  - Client authentication for web servers (e.g. eBay)
  - Access control to swimming pool, public library, civic amenity site
  - Age control (e.g. vending machines)
- eCommerce
  - Online account opening
  - Digital Rights Management
  - Qualified signature
- eHealth
  - Access to patient health record

Current Use Cases

- eGovernment:
  - Official document request: marital status, birth certificate, ...
  - Access to RNN database
- eTax:
  - Online tax form declaration and consultation

  - 2,2 million tax-on-web declarations in 2010
- eAccess
  - Client authentication for web servers (e.g. eBay)
  - Access control to swimming pool, public library, civic amenity site
  - Age control (e.g. vending machines)
- eCommerce
  - Online account opening
  - Digital Rights Management
  - Qualified signature
- eHealth
  - Access to patient health record

Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

Idea behind the e-ID Quick Key Toolset

KATHOLIEKE UNIVERSITEIT LEUVEN

Belgian e-ID is closed source and rigid $\Leftrightarrow$
Global e-ID deployment relatively young and still evolving
An open source implementation enables:

- Fast implementation of new functionalities for testing
- To get faster feedback on possible security risks through public scrutiny
- Parties other than the Belgian government to test/use the Belgian e-ID structure
- Easy access to a temporary e-ID token in case of theft/loss

See: `http://code.google.com/p/eid-quick-key-toolset/`

Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

Functionalities of the toolset

KATHOLIEKE UNIVERSITEIT LEUVEN

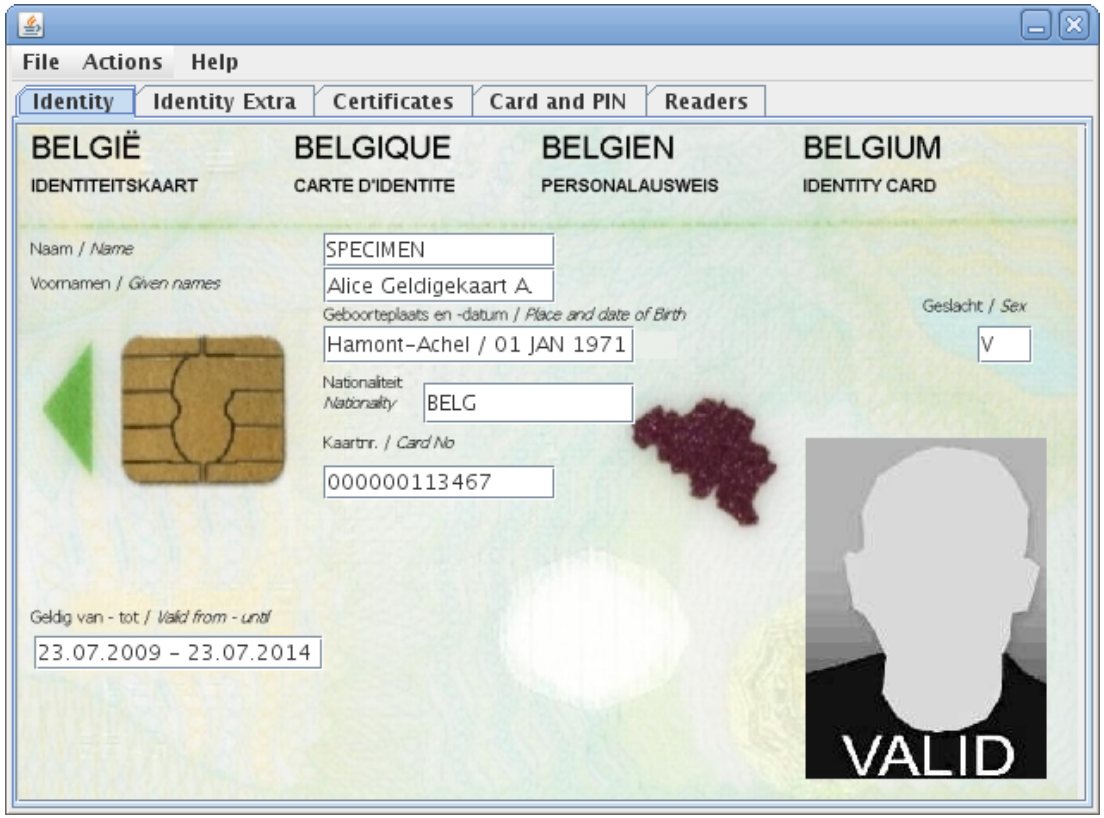
Next to the open source Java Card applet implementation of the Belgian e-ID, the e-ID quick key toolset also offers:

- e-ID data read functionality (not the private keys!)
- e-ID data modification
- Saving e-ID data in .xml file structure for later use
- Loading e-ID data previously stored in .xml format
- Write the e-ID applet to a set of supported empty Java Cards (non-exhaustive)
- Write previously read/loaded/modified data to the e-ID applet on this Java Card

Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

Demonstration



Outline

KATHOLIEKE UNIVERSITEIT LEUVEN

Mobile e-ID on Android Smart Phones

KATHOLIEKE UNIVERSITEIT LEUVEN

- Used G&D secure microSD card containing a Java Card
- Used open source Smart Card API found at
  `http://code.google.com/p/seek-for-android/`
- Same functionalities as the e-ID Quick Key Toolset, adapted to the mobile world:
  - Reading out Smart Card/e-ID
  - Storing data in .xml structure
  - Loading .xml files and automatically verify data validity using own e-ID
  - Sign data/files/mails

Mobile e-ID: one step further?

KATHOLIEKE UNIVERSITEIT LEUVEN

Having your e-ID data on your mobile phone of course has some major implications:

- No visual security measures can be implemented:
  - A JPEG could always be used to impersonate someone
  - The use of the authentication key could be mandatory during an identity check
  - How to implement this efficiently?
- What about malware on the phone OS?
- What are the new opportunities/use cases?
  - Two-factor authentication (phone + computer) easily implemented?
  - Extend e-ID for use in encrypted mobile communications, anonymous credentials, ...

Summary

KATHOLIEKE UNIVERSITEIT LEUVEN

- Short overview of the Belgian e-ID card
- Overview of our open source Belgian e-ID card implementation and toolset
- Preview of an e-ID implementation for mobile phones and future thoughts

Questions

KATHOLIEKE UNIVERSITEIT LEUVEN

?